IFW AF

TRANSMITTAL OF APPEAL BRIEF (Large Entity)	Docket No. EN998146

In Re Application Of: **Fetkovich et al.**

MAY 15 2006

Application No.	Filing Date	Examiner	Customer No.	Group Art Unit	Confirmation No.
09/443,204	11/18/1999	Patrick J.S. Santos	30400	2134	6903

Invention: **DYNAMIC ENCRYPTION AND DECRYPTION OF A STREAM OF DATA**

OIPE MAY 15 2006

COMMISSIONER FOR PATENTS:

Transmitted herewith is the Appeal Brief in this application, with respect to the Notice of Appeal filed on: **March 13, 2006**

The fee for filing this Appeal Brief is: **$500.00**

☐ A check in the amount of the fee is enclosed.

☐ The Director has already been authorized to charge fees in this application to a Deposit Account.

☒ The Director is hereby authorized to charge any fees which may be required, or credit any overpayment to Deposit Account No. 09-0457 (IBM) I have enclosed a duplicate copy of this sheet.

☐ Payment by credit card. Form PTO-2038 is attached.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

Kevin P. Radigan
Signature

Dated: May 12, 2006

Kevin P. Radigan, Esq.
Registration No.: 31,789

HESLIN ROTHENBERG FARLEY & MESITI, P.C.
5 Columbia Circle
Albany, New York 12203
Tel: (518) 452-5600
Fax: (518) 452-5579

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to "Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450" [37 CFR 1.8(a)] on May 12, 2006.
(Date)

Kevin P. Radigan
Signature of Person Mailing Correspondence

Kevin P. Radigan
Typed or Printed Name of Person Mailing Correspondence

05/17/2006 ZJUHAR1 00000003 090457 09443204
cc: 01 FC:1402 500.00 DA

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Appellants: Fetkovich et al. | Group Art Unit: 2134

Serial No.: 09/443,204 | Examiner: Santos Patrick J.D.

Filed: 11/18/99 | Appeal No.:

For: DYNAMIC ENCRYPTION AND DECRYPTION OF A STREAM OF DATA

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the U.S. Postal Service as first class mail in an envelope addressed to: Mail Stop Appeal Brief – Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on May 12, 2006.

Kevin P. Radigan
Kevin P. Radigan
Attorney for Appellants
Registration No. 31,789

Date of Signature: May 12, 2006.

Mail Stop Appeal Brief – Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Brief of Appellants

Dear Sir:

This is an appeal from a final rejection mailed December 29, 2005, rejecting claims 1, 2, 4, 5, 7-11, 13, 14, 16, 17, 19, 21-29, 31, 32, and 34-38, all the claims being considered in the above-identified application. This Brief is accompanied by a transmittal letter authorizing the charging of Appellants' deposit account for payment of the requisite fee set forth in 37 C.F.R. §1.17(c).

05/17/2006 ZJUHAR1 00000003 09443204
01 FC:1402 500.00 DA

Appellants' Brief is believed to be in compliance with the requirements set forth in 37 C.F.R. §41.37(c). However, if Appellants' Brief does not comply with the requirements set forth in 37 C.F.R. §41.37(c), Appellants request notification of the reasons for non-compliance and the opportunity to file an Amended Brief pursuant to 37 C.F.R. §41.37(d).

Real Party in Interest

This application is assigned to **International Business Machines Corporation** by virtue of an assignment executed by the inventors on October 13, 1999; October 14, 1999; and November 15, 1999, and recorded with the United States Patent and Trademark Office at reel 010405, frame 0321, on November 18, 1999. Therefore, the real party in interest is **International Business Machines Corporation**.

Related Appeals and Interferences

To the knowledge of the Appellants, Appellants' undersigned legal representative, and the assignee, there are no other pending appeals or interferences that will directly affect or be directly affected by or have a bearing on the Board's decision in the instant appeal. However, Appellants wish to bring to the attention of the Board their prior-issued Decision on Appeal mailed June 14, 2005 in connection with Appellants' prior appeal of the instant application, Appeal No. 2005-1192, a copy of which is attached herewith as noted in the Related Proceedings Appendix.

Status of Claims

This patent application was filed on November 18, 1999, with the U.S. Patent and Trademark Office. As filed, the application included 38 claims, of which four (4) were independent claims (i.e., claims 1, 14, 27, & 28).

In an initial Office Action dated September 25, 2003, claims 1-26, 35 and 38 were rejected under 35 U.S.C. §112, second paragraph, as indefinite for failing to particularly point out and distinctly claim the subject matter regarded as the invention. Additionally, claims 1, 2, 5-8, 12-19, 26 and 27 were rejected under 35 U.S.C. §102(b) as anticipated by Jones (U.S. Patent No. 5,412,730; hereinafter "Jones"); claim 28 was rejected under 35 U.S.C. §102(b) as anticipated by Warren et al. (U.S. Patent No. 5,719,937; hereinafter "Warren"); and claims 1, 13,

14 and 26 were rejected under 35 U.S.C. §102(b) as anticipated by Aucsmith et al. (U.S. Patent No. 5,991,403; hereinafter "Aucsmith"). In addition, claims 3, 9-11, 20 and 22-25 were rejected under 35 U.S.C. §103(a) as unpatentable over Jones in view of Nardone et al. (U.S. Patent No. 5,805,700; hereinafter "Nardone") and in further view of Leppek (U.S. Patent No. 5,933,501; hereinafter "Leppek"); claims 4 and 21 were rejected under 35 U.S.C. §103(a) as unpatentable over Jones in view of Nardone and Leppek and in further view of an article entitled "Digital Television Achieves Maturity" by Leonardo Chiariglione (hereinafter "Chiariglione"); claims 29 and 32-35 were rejected under 35 U.S.C. §103(a) as unpatentable over Jones in view of Warren; claims 30 and 36-38 were rejected under 35 U.S.C. §103(a) as unpatentable over Jones, Nardone and Leppek in view of Warren; and claim 31 was rejected under 35 U.S.C. §103(a) as unpatentable over Jones, Nardone, Leppek, and Chiariglione in view of Warren. In Appellants' response dated December 23, 2003, claims 1, 2, 4, 5, 7-14, 16-19, 21-29, 31, 32 & 34-38 were amended and claims 3, 6, 15, 20, 30 & 33 were cancelled (without prejudice).

In a final Office Action dated March 23, 2004, claims 1-3, 5-20 and 22-27 were rejected under 35 U.S.C. §103(a) as unpatentable over Jones in view of Nardone and further in view of Leppek; claims 1, 13, 14 and 26 were rejected under 35 U.S.C. §103(a) as unpatentable over Aucsmith in view of Nardone and Leppek; claims 4 and 21 were rejected under 35 U.S.C. §103(a) as unpatentable over Jones in view of Nardone and Leppek, and further in view of Chiariglione; claim 28 was rejected under 35 U.S.C. §103(a) as unpatentable over Warren in view of Nardone, and further in view of Leppek; claims 29-30 and 32-38 were rejected under 35 U.S.C. §103(a) as unpatentable over Jones in view of Warren, further in view of Nardone and Leppek; and, claim 31 was rejected under 35 U.S.C. §103(a) as unpatentable over Jones, Nardone, Leppek and Chiariglione in view of Warren. In Appellants' response dated May 17, 2004, no claims were amended.

A Notice of Appeal to the Board of Patent Appeals and Interferences was filed on June 23, 2004. In support of the Notice of Appeal, Appellants mailed an Appeal Brief on August 23, 2004, and responsive thereto an Examiner's Answer issued December 14, 2004. In reply to the Examiner's Answer, Appellants filed a Reply Brief on January 27, 2005 traversing various characterizations and conclusions contained in the Examiner's Answer at pages 36-44.

A Decision on Appeal was issued by the Board on June 14, 2005 reversing the Examiner's rejection on the appealed claims, but stating a new ground of rejection pursuant to 37 C.F.R. §41.50(b). Specifically, the prior-appealed claims were rejected by the Board under the first paragraph of 35 U.S.C. §112 for a lack of written description and lack of enablement for the prior-pending concept of dynamically changing "simultaneously" multiple encryption parameters.

Responsive to the Decision on Appeal, Appellants filed an Amendment on August 11, 2005, pursuant to 37 C.F.R. §41.50(b)(1). In this Amendment, independent claims 1, 14, 27 & 28 were amended, and claims 12 & 18 were canceled (without prejudice).

In a final Office Action mailed December 29, 2005, claims 1, 2, 5, 7-11, 13, 14, 16, 17, 19 & 22-27 were rejected under 35 U.S.C. §103(a) as being unpatentable over Jones in view of Nardone and further in view of Leppek. Claims 4 & 21 were rejected under 35 U.S.C. §103(a) as being unpatentable over Jones in view of Nardone and Leppek and further in view of Chiariglione; claims 28, 29, 32 & 34-38 were rejected under 35 U.S.C. §103(a) as being unpatentable over Jones in view of Warren, and further in view of Nardone and Leppek; and claim 31 was rejected under 35 U.S.C. §103(a) as being unpatentable over Jones, Nardone, Leppek and Chiariglione in view of Warren.

A Notice of Appeal to the Board of Appeals and Interferences was filed on March 15, 2006. The status of the claims is therefore as follows:

Claims allowed – none;
Claims objected to – none;
Claims rejected – 1, 2, 4, 5, 7-11, 13, 14, 16, 17, 19, 21-29, 31, 32 & 34-38; and
Claims canceled – 3, 6, 12, 15, 18, 20, 30 & 33.

Appellants are appealing the rejection of claims 1, 2, 4, 5, 7-11, 13, 14, 16, 17, 19, 21-29, 31, 32, and 34-38.

Status of Amendments

Appellants proffered no amendments responsive to the final Office Action dated December 29, 2005. The claims as set out in the Appendix include all prior entered claim amendments.

Summary of the Invention

In one aspect of the invention, Appellants claim a method (e.g., claim 1) for protecting a stream of data to be transferred between an encryption unit 20 (FIG. 1) and a decryption unit 32. The method includes encrypting the stream of data at the encryption unit for transferring of an encrypted stream of data from the encryption unit to the decryption unit (see, e.g., FIG. 1; page 14, lines 13^{+}). The encrypting of the stream of data is dynamically varied at the encryption unit over multiple portions of the stream of data (see, e.g., page 7, lines 22-25) by dynamically changing multiple encryption parameters employed for each portion of the stream of data (see, e.g., page 10, line 24 – page 14, line 28) and signaling the dynamic change in encryption parameters to the decryption unit (see, e.g., block 130 of FIG. 2; page 15, lines 1-18). The dynamically varying of the multiple encryption parameters employed for each portion of the stream of data is responsive to occurrence of a predefined condition in the stream of data (see, e.g., page 18, line 22 – page 19, line 17). Upon receipt of the encrypted data at the decryption unit, the technique includes decrypting the encrypted data, wherein the decrypting accounts for the dynamic varying of the encrypting by the encryption unit using the changed, multiple encryption parameters (see, e.g., page 15, line 19 – page 16, line 17).

In a further aspect of the invention, Appellants claim a system (e.g., claim 14) for protecting a stream of data. This system includes an encryption unit 20 (FIG. 1) and a decryption unit 32. The encryption unit encrypts the stream of data for transfer to the decryption unit (see, e.g., FIG. 1; page 14, lines 13^{+}). The system further includes means for dynamically varying the encrypting of the stream of data by the encryption unit over multiple portions of the stream of data (see, e.g., page 7, lines 22-25) by dynamically changing multiple encryption parameters employed by each portion of the stream of data (see, e.g., page 10, line 24 – page 14, line 28), and signaling the dynamic change in encryption parameters employed by each portion of the stream of data to the decryption unit (see, e.g., block 130 of FIG. 2; page 15, lines 1-18). The means for dynamically varying is responsive to occurrence of a predefined condition within the stream of data (see, e.g., page 18, line 22 – page 19, line 17). The decryption unit decrypts the encrypted data, and the decrypting accounts for the dynamic varying of the encrypting by the encryption unit using the dynamically changed, multiple encryption parameters (see, e.g., page 15, line 19 – page 16, line 17).

In a further aspect of the present invention, Appellants claim a system (e.g., claim 27) for protecting a stream of data to be transferred between a sender 12 (FIG. 1) and receiver 14. The system includes an encryption unit 20 disposed at the sender for encrypting the stream of data prior to transfer to the receiver (see, e.g., FIG. 1; page 14, lines 13^{+}). The encryption unit is adapted to dynamically vary the stream of data over multiple portions of the stream of data (see, e.g., page 7, lines 22-25) by dynamically changing multiple encryption parameters employed for each portion of the stream of data (see, e.g., page 10, line 24 – page 14, line 28) based on an occurrence of a predefined condition in the data stream (see, e.g., page 18, line 22 – page 19, line 17), and signaling the change in encryption parameters employed for each portion of the stream of data to the receiver (see, e.g., block 130 of FIG. 2; page 15, lines 1-18). The system further includes a decryption unit 32 disposed at the receiver for decrypting the encrypted data. The decryption unit is adapted to receive the changed encryption parameters to account for the dynamic varying of the encrypting by the encryption unit using the changed encryption parameters (see, e.g., page 15, line 19 – page 16, line 17).

In a still further aspect of the present invention, Appellants claim at least one program storage device (e.g., claim 28) readable by a machine, tangibly embodying at least one program of instructions executable by the machine (see, e.g., page 19, line 18 – page 20, line 2) to perform a method for protecting a stream of data to be transferred between an encryption unit 20 (FIG. 1) and decryption unit 32. The method performed includes encrypting the stream of data at the encryption unit for transfer thereof to the decryption unit (see, e.g., FIG. 1; page 14, lines 13^{+}); dynamically varying the encrypting of the stream of data at the encryption unit over multiple portions of the stream of data (see, e.g., page 7, lines 22-25) by dynamically changing multiple encryption parameters employed for each portion of the stream of data (see, e.g., page 10, line 24 – page 14, line 28) and signaling the change in encryption parameters to the decryption unit (see, e.g., block 130 of FIG. 2; page 15, lines 1-18), wherein the dynamically varying of the multiple encryption parameters employed by each portion of the stream of data is responsive to occurrence of a predefined condition in the stream of data (see, e.g., page 18, line 22 – page 19, line 17); and decrypting the encrypted data at the decryption unit, the decrypting accounting for the dynamic varying of the encrypting by the encryption unit using the dynamically changed, multiple encryption parameters (see, e.g., page 15, line 19 – page 16, line 17).

In another aspect, Appellants' technique includes multiplexing 24 (FIG. 1) the changed encryption parameters and the encrypted data at a sender 12 prior to transferring thereof to a receiver 14 containing the decryption unit 32 and demultiplexing of the changed encryption parameters and the encrypted data at the receiver (see, e.g., claims 4 & 31; and page 15, lines 1-18).

Grounds of Rejection to be Reviewed on Appeal

1. Whether claims 1, 2, 5, 7-11, 13, 14, 16, 17, 19 and 22-27 were rendered obvious under 35 U.S.C. §103(a) to one of ordinary skill in the art by Jones, Nardone and Leppek.

2. Whether claims 4 and 21 were rendered obvious under 35 U.S.C. §103(a) to one of ordinary skill in the art by Jones, Nardone, Leppek, and Chiariglione.

3. Whether claims 28, 29, 32 and 34-38 were rendered obvious under 35 U.S.C. §103(a) to one of ordinary skill in the art by Jones, Warren, Nardone and Leppek.

4. Whether claim 31 was rendered obvious under 35 U.S.C. §103(a) to one of ordinary skill in the art by Jones, Nardone, Leppek, Chiariglione and Warren.

Argument

I. ***Rejection under 35 U.S.C. §103(a) over U.S. Patent No. 5,412,730 (to Jones) in view of U.S. Patent No. 5,805,700 (to Nardone) and U.S. Patent No. 5,933,501 (to Leppek):***

Reversal of the rejection to claims 1, 2, 5, 7-11, 13, 14, 16, 17, 19 & 22-27 as obvious over Jones in view of Nardone and further in view of Leppek, is respectfully requested.

Appellants' invention provides a new technique for protecting a stream of data to be transferred between an encryption unit and a decryption unit. The technique includes dynamically varying the encrypting of the stream of data at the encryption unit over multiple portions of the stream of data. This dynamically varying is accomplished by dynamically changing multiple encryption parameters employed for each portion of the stream of data as the stream of data is passing through the encryption unit. This dynamically changing can occur periodically over time, for example, several times a second, thereby allowing only a small segment of the stream of data to be decoded should the encryption parameters used to encrypt that segment of data be uncovered. This concept of dynamically changing multiple encryption parameters employed for each portion of the stream of data as a stream of data is being encrypted is believed to comprise a unique approach from any of the applied art, which typically reply upon definition of a predefined policy for changing the encryption process.

Jones describes an encrypted data transmission system employing means for "randomly" altering the encryption keys. Pseudo-random number generators are employed at both the transmitting and receiving stations to supply identical sequences of encryption keys to a transmitting encoder and receiving decoder. An initial random number seed value is made available to both stations. The random number generators are advanced at times determined by predetermined characteristics of the data being transmitted so that, after transmission has taken place, the common encryption key can be known only to the transmitting and receiving stations.

A careful reading of Jones fails to uncover any teaching or suggestion of Appellants' concept of encrypting a stream of data and during the encryption process dynamically varying encrypting of the stream of data over multiple portions of the stream of data by dynamically changing multiple encryption parameters employed for each portion of the stream of data. The

Jones encryption approach requires pseudo-random binary sequence generation, and requires seed and mask values arranged at the sender and the receiver. Further, a change in Jones to the encryption process involves changing only an encryption key. The change in the encryption key occurs only at a predefined interval arranged *a priori* between the sender and the receiver. Jones changes the encryption key only when the counted number of bits or words or "items" matches the arranged interval. The disadvantage of this approach is that synchronization is absolutely essential. Bytes lost during transmission throw off the encryption/decryption process without any chance of recovery. In contrast, Appellants' invention of dynamically varying multiple encryption parameters employed for each portion of the stream of data as the stream of data is being encrypted ensures that only a small segment of the encrypted data could be exposed or lost should the encryption parameters used to encrypt that segment become uncovered or lost, respectively.

In addition, Appellants' recited process includes signaling the dynamic change in the encryption parameters from the encryption unit to the decryption unit. A careful reading of Jones fails to uncover any teaching or suggestion that the single encryption key change is signaled to the decryption unit. Rather, the patent teaches otherwise by describing a process which relies upon an *a priori* agreed upon process. In Jones, the decryption unit knows in advance where the encryption key change is to occur. In contrast, Appellants recite a truly dynamic varying of the encryption process wherein the dynamically changed encryption keys are forwarded from the encryption unit to the decryption unit.

At page 31 of the final Office Action, the Examiner states that Appellants' recited aspect of "signaling the dynamic change in the encryption parameters from the encryption unit to the decryption unit" is taught by Jones at Col. 1, lines 66 to Col. 2, line 7, wherein there is an alleged exchange of random number seed values and interval values between the encryptor and decryptor. Appellants respectfully submit that these lines of Jones disclose an *a priori* arrangement whereby the seed values and interval values are made available to both the transmitting station and a receiving station. Fig. 1 of Jones clearly shows that the interval number and random number seed are inputs to both stations. The transmitting station does not forward the interval number and seed number to the receiving station. Thus, there is no dynamic signaling of encryption parameter information *per se* from the encryption unit to the decryption

unit in Jones. In view of this, Appellants respectfully submit that the final Office Action mischaracterizes the teachings of Jones when asserting those teachings against Appellants' invention as recited in the independent claims presented.

Nardone is cited for allegedly teaching dynamically changing encryption parameters used to encrypt a stream of data (and presumably Appellants' recited concept of dynamically varying the encrypting over multiple portions of the stream of data by changing multiple encryption parameters employed for each portion of the stream of data). This characterization of the teachings of Nardone is respectfully traversed.

Nardone describes a policy-based selective encryption of compressed video data. Basic transfer units (BTUs) of compressed video data of a video image are selectively encrypted in Nardone in accordance with an encryption policy to degrade the video image to at least a virtually useless state, i.e., if the selectively encrypted compressed video image were to be rendered without decryption. In Nardone, an encryption policy refers to the encryption duty cycle. As stated at column 1, lines 40-59 thereof, Nardone achieves degradation that approximates the level provided by a total encryption approach, but requiring only a fraction of the processor cycle cost of the total encryption approach by selectively encrypting certain basic transfer units. This selective encryption occurs in Nardone at authoring time; and at authoring time, which basic transfer units are to be encrypted may be dynamically adjusted. As explained by Nardone, in one embodiment, where the video images are MPEG compressed, all BTUs containing either the start code for a group of pictures or the start code for a particular frame are encrypted, to prevent recovery of the video frames. In an alternate embodiment, a fraction of the BTUs of an I-frame, and a fraction of the BTUs of a P-frame are encrypted, again, to destroy data references by future frames. Thus, the goal of Nardone is to reduce the processor cycle cost required to entirely encrypt video data of video images. The dynamic adjustment of encryption policies in Nardone is taught to change which basic transfer units are to be encrypted (i.e., the duty cycle of the encryption process), and not the encryption process *per se*. This change in the amount of encryption being applied to the video data of the video images does not teach or suggest that multiple encryption parameters are changed between policies.

Thus, Nardone describes a change in encryption policies to effect the amount of partial encryption applied to video data of a video image in order to ensure sufficient degradation of the video image to a virtually useless state (if the selectively encrypted compressed video images were to be rendered without decryption), while requiring only a fraction of the processor cycle cost compared to a total encryption process. Because the policy selection at authoring time described by Nardone only presents a change in the duty cycle, i.e., a change in which basic transfer units of the video data are to be encrypted, Appellants respectfully submit that Nardone does not provide an insight as characterized in the final Office Action at page 29. The only "parameter" being changed with a dynamic adjustment in policy in Nardone is a change in the duty cycle of the encryption of the basic transfer units. The final Office Action points to no teaching or suggestion in Nardone that a change in encryption policy from one fractional encryption to another fractional encryption equates to dynamically changing multiple encryption parameters between different portions of the stream of data. To characterize the teachings of Nardone otherwise is believed to result from a hindsight reference to Appellants' own disclosure. It is noted at page 29 of the final Office Action that "while varying the degree of selective encryption in order to degrade video image is one possible encryption parameter to vary, it is not the only encryption parameter to vary." However, no section of Nardone is cited for supporting the alleged insight that multiple encryption parameters can be dynamically changed over multiple portions of a stream of data.

In apparent conflict to the above-cited insight with respect to Nardone, the final Office Action further acknowledges at the bottom of page 29 that Nardone is not explicit about setting multiple parameters in a policy. However, the final Office Action then alleges that the insight of Leppek is the application of multiple encryption operators at once. Again, Appellants respectfully submit that this insight is a hindsight mischaracterization of the teachings of Leppek, that is, to the extent deemed applicable to their claimed process.

Leppek describes a virtual encryption scheme which combines different encryption operators into a compound-encryption mechanism. The encryption "operators" in Leppek refer to different encryption "algorithms". For example, reference column 1, lines 54-56 where it is stated that a fundamental characteristic of essentially all encryption operators or <u>algorithms</u> is the fact that, given enough resources, almost any encryption algorithm can be broken. Thus, the

encryption operators in Leppek are encryption algorithms and do not equate to Appellants' recited encryption process wherein Appellants vary the encrypting over multiple portions of a stream of data by dynamically changing multiple encryption parameters employed for each portion of the stream of data.

In Leppek, data is first encoded using a first encryption operator (i.e., algorithm), then the same data is encoded using a second encryption operator, etc., thereby increasing the entropy of the data to make the encoded data look as random as possible. This approach is contrasted with Appellants' recited process wherein they dynamically change multiple encryption parameters employed for multiple portions of the stream of data while an encryption unit is encrypting a stream of data. In Appellants' approach, different segments of the stream of data are encrypted using different encryption parameters and there is a dynamic change in the encryption parameters such that the multiple encryption parameters employed for each portion of the stream of data change from one segment to another segment as the stream of data is passing through the encryption unit and being encrypted. In Leppek, there is a static, sequential application of a number of encryption algorithms (or encryption operators) *to the same segment of data*.

The final Office Action seeks to equate Leppek's teaching of a compound sequence of encryption operators, i.e., the sequential application of encryption algorithms, to Appellants' recited language of changing multiple encryption parameters employed for each portion of the stream of data during the dynamically varying of the encrypting of a stream of data. This conclusion is respectfully traversed. Leppek does not teach the application of multiple encryption operators to different portions of the streams of data. Rather, Leppek describes a sequential application of encryption algorithms to the same data to increase the entropy of the data. For example, reference column 4, lines 58-67 where Leppek teaches a successive process of accessing sequentially differing encryption operators (i.e., algorithms) and wrapping the previously encrypted data until the last access code in the encryption control sequence is processed. Clearly, the sequential application of encryption operators (i.e., algorithms) to the same data does not equate to the alleged insight of the application of multiple encryption operators being changed. First, the encryption operators described by Leppek are encryption algorithms, and do not equate to the encryption parameters recited in Appellants' encryption process. Secondly, there is no dynamic changing of multiple encryption parameters employed

for each of multiple portions of the stream of data in Leppek. Rather, Leppek expressly teaches the sequential application of encryption operators (i.e., algorithms) to the data so as to wrap the previously encrypted data with the next encryption operator algorithm.

For the above reasons, Appellants respectfully submit that the alleged insights drawn from Nardone and Leppek are a mischaracterization of the teachings of those patents, and therefore reconsideration and reversal of the obviousness rejection to their independent claims based upon Jones, Nardone and Leppek is requested.

Further, because Appellants' approach does not rely upon any predefined policy (such as in Jones), Appellants' process recites dynamically varying the encrypting of a stream of data at the encryption unit over multiple portions of the stream of data by dynamically changing multiple encryption parameters employed for each of multiple portions of the stream of data *and* signaling the dynamic change in encryption parameters to the decryption unit. Since the dynamic varying of the encrypting of the stream of data occurs at the encryption unit, the encryption unit signals the dynamic change to the decryption unit. Jones, Nardone and Leppek do not describe any mechanism for signaling dynamic changes in multiple parameters from an encryption unit to a decryption unit. In this regard, the final Office Action references at page 31 that Jones requires the exchange of random number seed values and interval values *between* the encryptor and the decryptor. (Jones, column 1, line 66 – column 2, line 7). This characterization of the teachings of Jones is respectfully traversed. In Jones, a seed value and interval value are established *a priori*, before an encryption process begins and are provided as inputs to both the encryption unit and the decryption unit as shown in FIG. 1 of Jones. Since they are provided *a priori* as inputs to both units, there is no signaling from the encryption unit to the decryption unit of the dynamic change of multiple encryption parameters. For this additional reason, Appellants allege error in rejecting their independent claims as obvious over the combination of Jones, Nardone and Leppek.

For at least the above-noted reasons, Appellants respectfully request reversal of the obviousness rejection to claims 1, 2, 5, 7-11, 13, 14, 16, 17, 19 & 22-27 based on Jones in view of Nardone and Leppek.

II. ***Rejection under 35 U.S.C. §103(a) over U.S. Patent No. 5,412,730 (to Jones), in view of U.S. Patent No. 5,805,700 (to Nardone), U.S. Patent No. 5,933,501 (to Leppek), and "Digital Television Achieves Maturity" by Chiariglione:***

Reversal of the rejection to claims 4 & 21 as obvious over Jones, Nardone, Leppek and Chiariglione is respectfully requested.

Dependent claims 4 & 21 further characterize independent claims 1 and 14, respectively, discussed above in connection with Argument I. Thus, these claims are believed allowable for the reasons stated above in connection their respective independent claim. Chiariglione is cited in the final Office Action for allegedly teaching multiplexing of various information into an encrypted bitstream. Without acquiescing to this characterization, Appellants note that Chiariglione does not teach or suggest the above-noted deficiencies of Jones, Nardone and Leppek when applied against their independent claims. Specifically, Chiariglione does not suggest dynamically varying the encrypting of the stream of data at the encryption unit over multiple portions of the stream of data by dynamically changing multiple encryption parameters employed for each portion of the stream of data. Further, Chiariglione does not teach signaling these dynamic changes in the multiple parameters from the encryption unit to the decryption unit by multiplexing the changed encryption parameters themselves with the encrypted data for transfer to the decryption unit.

For at least the above reasons, Appellants respectfully request reversal of the rejection to dependent claims 4 & 21 based on Jones, Nardone, Leppek and Chiariglione.

III. ***Rejection under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 5,412,730 (to Jones) in view of U.S. Patent No. 5,719,937 (to Warren), U.S. Patent No. 5,805,700 (to Nardone), and U.S. Patent No. 5,933,501 (to Leppek):***

Reversal of the rejection to claims 28, 29, 32 & 34-38 as obvious over Jones, Warren, Nardone and Leppek is respectfully requested.

Independent claim 28 is believed allowable for the same reasons stated above in connection with independent claims 1, 14 & 27 under Argument I. Warren is not believed to teach or suggest any of the above-noted deficiencies of Jones, Nardone and Leppek when applied against Appellants' independent claims. Warren is cited at pages 24 & 25 of the final Office Action for teaching a program storage device in an encrypting system. Without acquiescing to

this characterization of Warren, Appellants note that Warren does not teach or suggest the above-noted deficiencies of Jones, Nardone and Leppek when applied against the independent claims. Warren describes an encryption process using a scheme such as hidden data transport (HDT) and post-compression hidden data transport (PC-HDT). Warren describes certain advantages of using HDT and PC-HDT algorithms over other encoding technologies, but does not even describe switching between HDT and PC-HDT algorithms dynamically. Thus, Appellants respectfully submit that Warren is not relevant to the above-noted deficiencies of Jones, Nardone and Leppek when applied against the claims at issue.

Dependent claims 29, 32 & 34-38 are believed allowable over the combination of Jones, Warren, Nardone and Leppek for the same reasons stated hereinabove for independent claim 28 from which they directly or ultimately depend, as well as for their own additional characterizations.

For at least these reasons, Appellants respectfully request reversal of the obviousness rejection to claims 28, 29, 32 & 34-38 based on Jones in view of Warren, Nardone and Leppek.

IV. ***Rejection under 35 U.S.C. §103(a) over U.S. Patent No. 5,832,526 (to Jones), in view of U.S. Patent No. 5,805,700 (to Nardone), U.S. Patent No. 5,933,501 (to Leppek), "Digital Television Achieves Maturity" by Chiariglione, and U.S. Patent No. 5,719,937 (to Warren):***

Reversal of the rejection to claim 31 as obvious over Jones, Nardone, Leppek, Chiariglione and Warren is respectfully requested.

Dependent claim 31 is believed allowable for the same reasons as independent claim 28 from which it depends, as well as for its own additional characterizations. As noted above in connection with Argument II, Chiariglione is not believed to teach or suggest the noted deficiencies of Jones, Nardone, Leppek and Warren when applied against Appellants' independent claims, and more specifically, independent claim 28. None of the applied teachings, taken singularly or in combination, suggest Appellants' dynamic encoding technique which includes dynamically varying the encrypting of the stream of data at the encryption unit over multiple portions of the stream of data by dynamically changing multiple encryption parameters employed for each portion of the stream of data.

Thus, for the reasons stated above, Appellants request reversal of the rejection to dependent claim 31 based upon the combination of Jones, Nardone, Leppek, Chiariglione and Warren.

Conclusion

Appellants respectfully request reversal of the rejections set forth in the final Office Action. Appellants submit that their claimed invention would not have been rendered obvious by Jones, Nardone, Leppek, Chiariglione and Warren. These patents do not, individually or in combination, teach or suggest Appellants' encrypting process which includes dynamically varying the encrypting of the stream of data at the encryption unit over multiple portions of the stream of data by dynamically changing multiple encryption parameters employed for each portion of the stream of data, and signaling the dynamic change in encryption parameters to the decryption unit.

Accordingly, reversal of all rejections is respectfully requested.

Respectfully submitted,

Kevin P. Radigan

Kevin P. Radigan
Reg. No. 31,789
Attorney for Appellants

Dated: May 12, 2006

HESLIN ROTHENBERG FARLEY & MESITI, P.C.
5 Columbia Circle
Albany, New York 12203
Telephone: (518) 452-5600
Facsimile: (518) 452-5579

Claims Appendix

1. A method for protecting a stream of data to be transferred between an encryption unit and a decryption unit, said method comprising:

encrypting the stream of data at said encryption unit for transferring of said encrypted stream of data from said encryption unit to said decryption unit;

dynamically varying said encrypting of said stream of data at said encryption unit over multiple portions of the stream of data by dynamically changing multiple encryption parameters employed for each portion of the stream of data and signaling said dynamic change in encryption parameters to said decryption unit, said dynamically varying of said multiple encryption parameters employed for each portion of the stream of data being responsive to occurrence of a predefined condition in said stream of data; and

decrypting said encrypted data at the decryption unit, said decrypting accounting for said dynamic varying of said encrypting by said encryption unit using said dynamically changed, multiple encryption parameters.

2. The method of claim 1, wherein said multiple encryption parameters comprise at least two of an encryption key, an encryption granularity, an encryption density scale, an encryption density, an encryption delay, an encryption key update variable, and an encryption key update data trigger.

3. Canceled.

4. The method of claim 2, further comprising multiplexing said changed encryption parameters and said encrypted data at a sender prior to transferring thereof to a receiver containing said decryption unit, and demultiplexing said changed encryption parameters and said encrypted data at said receiver.

5. The method of claim 1, wherein said dynamically varying comprises dynamically varying said multiple encryption parameters based on passage of a predefined number of units of physical data or passage of a predefined number of conceptual units of data.

6. Canceled.

7. The method of claim 1, wherein said stream of data comprises a stream of compressed data, and wherein said method further comprises decompressing said compressed data after said decrypting of said encrypted data by said decryption unit.

8. The method of claim 7, wherein said stream of compressed data comprises one of MPEG encoded video data, MPEG encoded audio data, and Dolby AC-3 audio data.

9. The method of claim 1, further comprising initializing a plurality of encryption parameters based on a sensitivity of said stream of data, said plurality of encryption parameters being employed by said encrypting and wherein said changed multiple encryption parameters of said dynamically varying comprise multiple encryption parameters of said plurality of encryption parameters.

10. The method of claim 1, wherein said stream of data comprises a stream of MPEG compressed data, and said method further comprises setting a plurality of encryption parameters for use by said encrypting based upon sensitivity of said stream of MPEG compressed data, and wherein said changed multiple encryption parameters comprise multiple encryption parameters of said plurality of encryption parameters.

11. The method of claim 10, wherein said setting of said plurality of encryption parameters includes establishing at least two of an encryption granularity, an initial encryption key, a density scale, a density, an encryption delay, and a key update data trigger for said stream of MPEG encoded data.

12. Canceled.

13. The method of claim 1, wherein said dynamically varying comprises dynamically varying said multiple encryption parameters responsive to passage of a predefined number of data bits in said stream of data, or alternatively, responsive to passage of a predefined number of data units in said stream of data, wherein said data units comprise at least one of a program, a sequence, a group of pictures, a picture, a slice, or a macroblock.

14. A system for protecting a stream of data comprising:

an encryption unit and a decryption unit, the encryption unit encrypting the stream of data for transfer to the decryption unit;

means for dynamically varying said encrypting of said stream of data by said encryption unit over multiple portions of the stream of data by dynamically changing multiple encryption parameters employed by each portion of the stream of data and signaling said dynamic change in encryption parameters employed by each portion of the stream of data to said decryption unit, said means for dynamically varying being responsive to occurrence of a predefined condition in said stream of data; and

wherein said decryption unit decrypts said encrypted data, said decrypting accounting for said dynamic varying of said encrypting by said encryption unit using said dynamically changed, multiple encryption parameters.

15. Canceled.

16. The system of claim 14, wherein said stream of data comprises a stream of digital data.

17. The system of claim 14, wherein said means for dynamically varying comprises means for dynamically varying said multiple encryption parameters based on passage of a predefined number of units of physical data or passage of a predefined number of conceptual units of data.

18. Canceled.

19. The system of claim 14, wherein said multiple encryption parameters comprise at least two of an encryption key, an encryption granularity, an encryption density scale, an encryption density, an encryption delay, an encryption key update variable, and an encryption key update data trigger.

20. Canceled.

21. The system of claim 14, further comprising a data multiplexer for multiplexing said changed encryption parameters into said encrypted data for transfer thereof to said decryption unit.

22. The system of claim 14, further comprising means for setting a plurality of encryption parameters based on sensitivity of said stream of data, said plurality of encryption parameters being employed by said encryption unit and wherein said changed multiple encryption parameters comprise encryption parameters of said plurality of encryption parameters.

23. The system of claim 22, wherein said stream of data comprises a stream of compressed data, and wherein said system further comprises a decoder for decompressing said compressed data after decrypting thereof by said decryption unit.

24. The system of claim 23, wherein said stream of compressed data comprises a stream of one of MPEG encoded video data, MPEG encoded audio data, and Dolby AC-3 audio data.

25. The system of claim 22, wherein said means for setting said plurality of encryption parameters includes means for establishing at least two of an encryption granularity, an encryption key, a density scale, a density, an encryption delay, and a key update data trigger.

26. The system of claim 14, wherein said means for dynamically varying comprises means for changing said multiple encryption parameters based on a predefined number of bits being encoded by said encryption unit, or alternatively, based on a predefined number of units being encoded by said encryption unit, said units comprising one of a program, a sequence, a group of pictures, a picture, a slice, or a macroblock.

27. A system for protecting a stream of data to be transferred between a sender and a receiver, said system comprising:

an encryption unit disposed at said sender for encrypting the stream of data prior to transfer to said receiver, said encryption unit being adapted to dynamically vary encrypting of the stream of data over multiple portions of the stream of data by dynamically changing multiple encryption parameters employed for each portion of the stream of data based on an occurrence of a predefined condition in said data stream and signaling said change in encryption parameters employed for each portion of the stream of data to said receiver; and

a decryption unit disposed at said receiver for decrypting said encrypted data, said decryption unit being adapted to receive said changed encryption parameters to account for said dynamic varying of said encrypting by said encryption unit using said changed encryption parameters.

28. At least one program storage device readable by a machine, tangibly embodying at least one program of instructions executable by the machine to perform a method for protecting a stream of data to be transferred between an encryption unit and a decryption unit, comprising;

encrypting the stream of data at said encryption unit for transfer thereof to said decryption unit;

dynamically varying said encrypting of said stream of data at said encryption unit over multiple portions of the stream of data by dynamically changing multiple encryption parameters employed for each portion of the stream of data and signaling said change in encryption parameters to said decryption unit, wherein said dynamically varying of said multiple encryption parameters employed for each portion of the stream of data is responsive to occurrence of a predefined condition in said stream of data; and

decrypting said encrypted data at the decryption unit, said decrypting accounting for said dynamic varying of said encrypting by said encryption unit using said dynamically changed, multiple encryption parameters.

29. The at least one program storage device of claim 28, wherein said multiple encryption parameters comprise at least two of an encryption key, an encryption granularity, an encryption density scale, an encryption density, an encryption delay, an encryption key update variable, and an encryption key update data trigger.

30. Canceled.

31. The at least one program storage device of claim 29, wherein said method further comprises multiplexing said changed encryption parameters and said encrypted data at a sender prior to transferring thereof to a receiver containing said decryption unit, and demultiplexing said changed encryption parameters and said encrypted data at said receiver.

32. The at least one program storage device of claim 28, wherein said dynamically varying comprises dynamically varying said multiple encryption parameters based on passage of a predefined number of units of physical data or passage of a predefined number of conceptual units of data.

33. Canceled.

34. The at least one program storage device of claim 28, wherein said stream of data comprises a stream of compressed data, and wherein said method further comprises decompressing said compressed data after said decrypting of said encrypted data by said decryption unit.

35. The at least one program storage device of claim 34, wherein said stream of compressed data comprises one of MPEG encoded video data, MPEG encoded audio data, and Dolby AC-3 audio data.

36. The at least one program storage device of claim 28, wherein said method further comprises initializing a plurality of encryption parameters based on sensitivity of said stream of data, said plurality of encryption parameters being employed by said encrypting and wherein said changed multiple encryption parameters of said dynamically varying comprise multiple encryption parameters of said plurality of encryption parameters.

37. The at least one program storage device of claim 28, wherein said stream of data comprises a stream of MPEG compressed data, and said method further comprises setting a plurality of encryption parameters for use by said encrypting based upon sensitivity of said stream of MPEG compressed data, and wherein said changed multiple encryption parameters comprise multiple encryption parameters of said plurality of encryption parameters.

38. The at least one program storage device of claim 37, wherein said setting of said plurality of encryption parameters includes establishing at least two of an encryption granularity, an initial encryption key, a density scale, a density, an encryption delay, and a key update data trigger for said stream of MPEG encoded data.

* * * * *

Evidence Appendix

None.

Related Proceedings Appendix

Attached herewith is a Decision on Appeal mailed June 14, 2005, by the United States Patent and Trademark Office Board of Patent Appeals and Interferences in connection with Appeal No. 2005-1192.

The opinion in support of the decision being entered today was not written for publication and is not binding precedent of the Board.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte JOHN EDWARD FETKOVICH, WAI MAN LAM, and
GEORGE WILLIAM WILHELM JR.

Appeal No. 2005-1192
Application No. 09/443,204

ON BRIEF

MAILED

JUN 14 2005

U.S. PATENT AND TRADEMARK OFFICE
BOARD OF PATENT APPEALS
AND INTERFERENCES

Before HAIRSTON, RUGGIERO and DIXON, Administrative Patent Judges.

HAIRSTON, Administrative Patent Judge.

DECISION ON APPEAL

This is an appeal from the final rejection of claims 1, 2, 4, 5, 7 through 14, 16 through 19, 21 through 29, 31, 32 and 34 through 38.

The disclosed invention relates to a method and system for dynamically varying the encryption of a stream of data by an encryption unit by dynamically changing simultaneously multiple encryption parameters, and for taking into account the

dynamically changed, multiple encryption parameters during the decryption of the encrypted data by the decryption unit.

Claim 1 is illustrative of the claimed invention, and it reads as follows:

> 1. A method for protecting a stream of data to be transferred between an encryption unit and a decryption unit, said method comprising:
>
> encrypting the stream of data at said encryption unit for transferring of said encrypted stream of data from said encryption unit to said decryption unit;
>
> dynamically varying said encrypting of said stream of data at said encryption unit by dynamically changing simultaneously multiple encryption parameters and signaling said dynamic change in encryption parameters to said decryption unit, said dynamically varying of said multiple encryption parameter being responsive to occurrence of a predefined condition in said stream of data; and
>
> decrypting said encrypted data at the decryption unit, said decrypting accounting for said dynamic varying of said encrypting by said encryption unit using said dynamically changed, multiple encryption parameters.

The references relied on by the examiner are:

Jones	5,412,730	May 2, 1995
Warren et al. (Warren)	5,719,937	Feb. 17, 1998
Nardone et al. (Nardone)	5,805,700	Sep. 8, 1998
Leppek	5,933,501	Aug. 3, 1999
Aucsmith et al. (Aucsmith)	5,991,403	Nov. 23, 1999 (filed Dec. 23, 1996)

Chiariglione, "Digital Television Achieves Maturity," 21st Impact - Opima, at http://www.vxm.com/impact.opima.html (last visited on Sep. 13, 2003)(hereinafter referred to as Chiariglione).

Claims 1, 2, 5, 7 through 14, 16 through 19 and 22 through 27 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Jones in view of Nardone and Leppek.

Claims 1, 13, 14 and 26 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Aucsmith in view of Nardone and Leppek.

Claims 4 and 21 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Jones in view of Nardone, Leppek and Chiariglione.

Claim 28 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Warren in view of Nardone and Leppek.

Claims 29, 32 and 34 through 38 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Jones in view of Warren, Nardone and Leppek.

Claim 31 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Jones in view of Nardone, Leppek, Chiariglione and Warren.

Reference is made to the briefs and the answer for the respective positions of the appellants and the examiner.

OPINION

The rejections of record are hereby reversed, and a new ground of rejection is entered under 37 CFR § 41.50(b) as to all of the claims on appeal.

All of the claims on appeal require "dynamically changing simultaneously multiple encryption parameters." The examiner acknowledges (answer, pages 6, 27 and 32) that the primary references to Jones, Aucsmith and Warren, respectively, all fail to teach the quoted limitation found in all of the claims on appeal. The examiner turns to Nardone for a teaching of "dynamically changing encryption parameters" (answer, page 6), but Nardone's teaching (column 1, lines 51 through 59; column 4, lines 23 through 34) of dynamically adjusting encryption policy is not described in the context of "dynamically changing simultaneously multiple encryption parameters." Leppek allegedly "teaches setting multiple parameters" (answer, page 6), but, instead of performing any encryption operations "simultaneously," all encryption in Leppek is performed "sequentially" or "successively" (Abstract). The multiplexing teachings of Chiariglione do not cure any of the noted shortcomings in the teachings of Jones, Nardone and Leppek.

In summary, all of the obviousness rejections of claims 1, 2, 4, 5, 7 through 14, 16 through 19, 21 through 29, 31, 32 and 34 through 38 are reversed.

The following new rejection of claims 1, 2, 4, 5, 7 through 14, 16 through 19, 21 through 29, 31, 32 and 34 through 38 is entered under the provisions of 37 CFR § 41.50(b):

Claims 1, 2, 4, 5, 7 through 14, 16 through 19, 21 through 29, 31, 32 and 34 through 38 are rejected under the first paragraph of 35 U.S.C. § 112 for lack of written description and lack of enablement. Neither the originally filed disclosure nor the originally filed claims sets forth dynamically changing "simultaneously" multiple encryption parameters. The originally filed disclosure (Abstract; page 4, lines 16 through 22; page 7, lines 22 through 25; page 13, lines 22 through 26; page 14, line 18 through page 15, line 8; page 19, lines 5 through 8) mentions dynamically changing parameters, but not "simultaneously." Thus, the claims are rejected for lack of written description. The claims are also rejected for lack of enablement because the skilled artisan would have to resort to undue experimentation to arrive at a system and method that is capable of dynamically changing "simultaneously" multiple encryption parameters.

Appellants' disclosure is of little help to the artisan because it is completely silent as to such a teaching.

DECISION

The decision of the examiner rejecting claims 1, 2, 4, 5, 7 though 14, 16 through 19, 21 through 29, 31, 32 and 34 through 38 under 35 U.S.C. § 103(a) is reversed.

This decision contains a new ground of rejection pursuant to 37 CFR § 41.50(b) (effective September 13, 2004, 69 Fed. Reg. 49960 (August 12, 2004), 1286 Off. Gaz. Pat. Office 21 (September 7, 2004)). 37 CFR § 41.50(b) provides "[a] new ground of rejection pursuant to this paragraph shall not be considered final for judicial review."

37 CFR § 41.50(b) also provides that the appellant, WITHIN TWO MONTHS FROM THE DATE OF THE DECISION, must exercise one of the following two options with respect to the new ground of rejection to avoid termination of the appeal as to the rejected claims:

> (1) Reopen prosecution. Submit an appropriate amendment of the claims so rejected or new evidence relating to the claims so rejected, or both, and have the matter reconsidered by the examiner, in which event the proceeding will be remanded to the examiner . . . .

(2) Request rehearing. Request that the proceeding be reheard under § 41.52 by the Board upon the same record . . . .

REVERSED - 37 CFR § 41.50(b)

KENNETH W. HAIRSTON Administrative Patent Judge	)	
JOSEPH F. RUGGIERO Administrative Patent Judge	)	BOARD OF PATENT APPEALS AND INTERFERENCES
JOSEPH L. DIXON Administrative Patent Judge	)	

KWH/hh

HESLIN, ROTHENBERG, FARLEY & MESITI, P.C.
5 COLUMBIA CIRCLE
ALBANY, NY 12203